

# SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

## ***INTERCONNECTING DEVICE, COMPUTER READABLE MEDIUM, AND COMMUNICATION SETTING METHOD***

### Cross Reference to Related Applications

This patent application claims priority from a Japanese patent application, No. 2001-253225 filed on August 23, 2001, the contents of which are incorporated herein by reference.

### Background of Invention

#### Field of the Invention

[0001] The present invention relates to an interconnecting device, a computer readable medium, and a communication setting method. More particularly, the present invention relates to an interconnecting device for setting a communication setting of a computer network.

#### Description of the Related Art

[0002] Conventionally, security against illegal access from unauthorized computers into a computer network has been built using a management server which generally manages the computer network. For example, access to the computer network is restricted by user authentication by the management server, VLAN setting or the like.

[0003] However, in a conventional computer network system, since the management server restricts access to the computer network, any computer operated by a user

connects to the management server via the computer network. Consequently, there is no means to restrict access to the computer network from almost any computer, and there is a problem that any computer is readily allowed to enter the communication through the computer network.

## Summary of Invention

- [0004] Therefore, it is an object of the present invention to provide an interconnecting device, a communication setting program, and a communication setting method, which are capable of overcoming the above drawbacks accompanying the conventional art. The above and other objects can be achieved by combinations described in the independent claims. The dependent claims define further advantageous and exemplary combinations of the present invention.
- [0005] According to the first aspect of the present invention, an interconnecting device, which interconnects communication in a computer network, is provided. The interconnecting device includes a first holding unit which holds a removable nonvolatile memory, a reading unit which reads a first device identifier of a first communication device, which is allowed to communicate in a computer network, from a nonvolatile memory held by the first holding unit, and a setting unit which sets a communication setting of computer network to allow the first communication device identified by the first device identifier to communicate in the computer network.
- [0006] The nonvolatile memory may store the encrypted first device identifier and the interconnecting device may further include a decoder which decodes the encrypted first device identifier read by the reading unit. The setting unit may set the interconnecting device to allow the first communication device identified by the first device identifier to communicate in the interconnecting device. The setting unit may further set a bandwidth of communication of the first communication device, identified by the first device identifier, in the interconnecting device.
- [0007] The interconnecting device may further include a transmitting unit which transmits the first device identifier to another interconnecting device, which connects to the interconnecting device, to set to allow the first communication device identified by the first device identifier to communicate in the other interconnecting device.

- [0008] The other interconnecting device connects the computer network and another computer network. The transmitting unit may transmit the first device identifier to the other interconnecting device to allow the first communication device identified by the first device identifier to communicate in the other computer network.
- [0009] The interconnecting device may further include a transmitting unit which transmits the first device identifier to a management apparatus, which manages the computer network, so as to set to allow the first communication device identified by the first device identifier to communicate in the computer network.
- [0010] The interconnecting device may further include a second holding unit which holds a removable nonvolatile memory. The reading unit may read a second device identifier of a second communication device, which is allowed to communicate in the computer network, from the nonvolatile memory held by the second holding unit. The setting unit may set a communication setting of the computer network to allow the second communication device identified by the second device identifier to communicate in the computer network.
- [0011] The setting unit may set the interconnecting device to allow the first communication device identified by the first device identifier to communicate in the interconnecting device. The setting unit may also set the interconnecting device to allow the second communication device identified by the second device identifier to communicate in the interconnecting device.
- [0012] The interconnecting device may further include a first connection port to which the first communication device connects and a second connection port to which the second communication device connects. The setting unit may set the interconnecting device to allow communication of the first communication device at the first connection port and the second communication device at the second connection port. The setting unit may further set a bandwidth of communication at the first connection port and the second connection port.
- [0013] The interconnecting device may further include a storage unit which stores a device identifier of at least one of the communication devices, the device identifier allowing the communication device to communicate in the interconnecting device, and

a communication controller which restricts access to the interconnecting device from a communication device which is not allowed to communicate in the interconnecting device, based on the device identifier stored in the storage unit.

[0014] The setting unit may store the storage unit with the first device identifier read by the reading unit to allow the first communication device identified by the first device identifier read by the reading unit to communicate in the interconnecting device.

[0015] The interconnecting device may include a plurality of connection ports to which a plurality of communication devices connect correspondingly and the storage unit may store a device identifier of at least one of the communication devices, the device identifier allowing the communication device to communicate at a corresponding connection port out of the plurality of connection ports, which correspond to a plurality of communication devices respectively.

[0016] The second aspect of the present invention provides a communication setting program for an interconnecting device, which sets a communication setting of a computer network. The communication setting program includes a reading module which allows the interconnecting device to read a device identifier of a communication device, which is allowed to communicate in the computer network, from a removable nonvolatile memory. The communication setting program also includes a setting module which allows the interconnecting device to set a communication setting of the computer network to allow a communication device identified by a device identifier to communicate in the computer network.

[0017] The setting module may set the interconnecting device to allow a communication device identified by a device identifier to communicate in the interconnecting device.

[0018] The communication setting program may further include a transmitting module which allows the interconnecting device to transmit a device identifier to another interconnecting device, connecting to the interconnecting device, to set to allow a communication device identified by the device identifier to communicate in the other interconnecting device.

[0019] The third aspect of the present invention provides a communication setting method of a computer network by an interconnecting device, which interconnects

communication in the computer network. The communication setting method includes steps of holding a removable nonvolatile memory, reading a device identifier of a communication device, which is allowed to communicate in the computer network, from the held nonvolatile memory, and setting a communication setting of the computer network to allow the communication device identified by the device identifier to communicate in the computer network.

[0020] This summary of the present invention does not necessarily describe all necessary features so that the invention may also be a sub-combination of these described features.

### Brief Description of Drawings

[0021] Fig. 1 shows a configuration of a computer network 100.

[0022] Fig. 2 shows a configuration of an interconnecting device 10a.

[0023] Fig. 3 shows a data format of a communication control file stored in a storage unit 110.

[0024] Fig. 4 shows a configuration of the computer network 100 and a computer network 200.

[0025] Fig. 5 shows hardware components in a management apparatus 20.

### Detailed Description

[0026] The invention will now be described based on preferred embodiments, which do not intend to restrict the scope of the present invention, but rather to exemplify the invention. All of the features and the combinations thereof described in the embodiments are not necessarily essential to the invention.

[0027] Fig. 1 shows a configuration of a computer network 100 according to one embodiment of the present invention. The computer network 100 of the present embodiment includes interconnecting devices 10a and 10b, such as switching hubs, which interconnect communication in the computer network 100, a management apparatus 20 which manages communication in the computer network 100, and communication devices 30a, 30b, 30c and 30d which are in communication in the

computer network 100.

[0028] The interconnecting devices 10a and 10b read setting information of the computer network 100 from a nonvolatile memory, such as an IC card, a Miniature card, a diskette or the like, and set a communication setting of the computer network 100. For example, the interconnecting device 10a includes an IC card slot, which are an example of a holding unit to hold a nonvolatile memory, and reads a media access control address (MAC address), as a device identifier of the communication device 30a, from an IC card inserted into the IC card slot by a user of the communication device 30a. Then the interconnecting device 10a set the interconnecting device 10a to allow the communication device 30a identified by the MAC address read from the IC card to communicate in the interconnecting device 10a.

[0029] A user of the communication device 30a inserts the IC card into the interconnecting device 10a. The MAC address of the communication device 30a, as an ID to connect the communication device 30a to the computer network 100, is stored in the IC card. Then the user is allowed to log into the computer network 100 from the communication device 30a when the IC card is inserted into the interconnecting device 10a. When the IC card is removed from the interconnecting device 10a, access to the computer network 100 from the communication device 30a is restricted. For example, the user may be prohibited to log into the computer network 100 from the communication device 30a, or only a certain operation, such as accessing to data in the communication devices 30b, 30c or 30d from the communication device 30a, may be allowed.

[0030] The interconnecting device 10a transmits the MAC address read from the IC card to the interconnecting device 10b to allow the communication device 30a identified by the MAC address read from the IC card to communicate in the interconnecting device 10b. Then the interconnecting device 10b sets the interconnecting device 10b to allow the communication device 30a identified by the MAC address received from the interconnecting device 10a to communicate in the interconnecting device 10b. In other words, a user of the communication device 30a is allowed to communicate with the communication devices 30c and 30d connected to the interconnecting device 10b from the communication device 10a by inserting the IC card, in which the MAC

address for identifying the communication device 30a is stored, into the interconnecting device 10a.

[0031] In another example, the interconnecting device 10a transmits the MAC address read from the IC card to the management apparatus 20 to allow the communication device 30a identified by the MAC address read from the IC card to communicate in the computer network 100. Then the management apparatus 20 sets the interconnecting device 10a and 10b to allow the communication device 30a identified the MAC address received from the interconnecting device 10a to communicate in the computer network 100. Then a user of the communication device 30a is allowed to communicate in the computer network 100 from the communication device 30a by inserting the IC card, in which the MAC address for identifying the communication device 30a is stored, into the interconnecting device 10a.

[0032] According to the interconnecting devices 10a and 10b of the present embodiment, a designated user has the designated IC card, which is an ID to log into the computer network 100 from a designated communication device operated by the designated user, so that only the designated user who has the designated IC card can be allowed to log into the computer network 100 from the designated communication device. Therefore, illegal access into the computer network 100 can be prevented since only the designated user, who has both the designated communication device and the designated IC card, is allowed to log into the computer network 100.

[0033] According to the computer network 100 of the present embodiment, it is possible to prohibit access into the management apparatus 20 from a communication device which is not allowed to communicate in the interconnecting devices 10a and 10b, since access into the computer network 100 from the communication devices 30a, 30b, 30c and 30d can be restricted at the interconnecting devices 10a and 10b. Therefore, the computer network 100 of the present embodiment can build a computer network system with high security against illegal access.

[0034] Fig. 2 shows a configuration of the interconnecting device 10a of the present embodiment. Since configurations of the interconnecting device 10a and the interconnecting device 10b are substantially identical, a configuration and operation of merely the interconnecting device 10a will be described hereinafter.

[0035] The interconnecting device 10a includes holding units 102a, 102b, 102c, 102d, 102e and 102f, a reading unit 104, a decoder 106, a setting unit 108, a storage unit 110, a communication unit 112, a communication controller 114, and connection ports 116a, 116b, 116c, 116d, 116e and 116f. The holding units 102a, 102b, 102c, 102d, 102e and 102f hold removable nonvolatile memories. The reading unit 104 reads a device identifier of a communication device from the nonvolatile memory. The decoder 106 decodes the encrypted device identifier. The setting unit 108 sets communication setting of the computer network 100 to allow the communication device identified by the device identifier to communicate in the computer network 100. The storage unit 110 stores a device identifier of at least one of communication devices, which is allowed to communicate in the interconnecting device 10a. The communication unit 112 transmits and receives a device identifier. The communication controller 114 restricts access to the interconnecting device 10a from a communication device which is not allowed to communicate in the interconnecting device. The connection ports 116a, 116b, 116c, 116d, 116e and 116f connect to the respective communication devices 30a, 30b, 30c or 30d.

[0036] The holding units 102a, 102b, 102c, 102d, 102e and 102f hold nonvolatile memories in which device identifiers of communication devices are stored. Then the reading unit 104 reads the device identifier of the communication device, which is allowed to communicate in the computer network 100, from the nonvolatile memory held by the holding units 102a, 102b, 102c, 102d, 102e or 102f. The decoder 106 decodes the device identifier in the case that the device identifier read from the nonvolatile memory is encrypted. Then the decoder 106 supplies the decoded device identifier to the setting unit 108.

[0037] The setting unit 108 sets a communication setting of the computer network 100 to allow a communication device identified by a device identifier read from a nonvolatile memory to communicate in the computer network 100. The setting unit 108 sets the interconnecting device 10a to allow a communication device identified by a device identifier read from a nonvolatile memory to communicate in the interconnecting device 10a. Specifically, the setting unit 108 allows a communication device identified by a device identifier read from a nonvolatile memory to communicate in the interconnecting device 10a by storing in the storage unit 110 the



device identifier read from the nonvolatile memory.

[0038] Then the communication controller 114 restricts access to the interconnecting device 10a from a communication device, which is not allowed to communicate in the interconnecting device, based on the device identifier stored in the storage unit 110. In other words, the communication controller 114 allows the communication device identified by the device identifier read from a nonvolatile memory and stored in the storage unit 110 to communicate in the interconnecting device 10a. For example, the communication controller 114 refers to header information of data received by the communication unit 112 and allows the communication unit 112 to transmit the data when the device identifier of the communication device in the header information is consistent with the device identifier stored in the storage unit 110.

[0039] The communication unit 112 receives a device identifier of a communication device, the device identifier allowing the communication device to communicate in the interconnecting device 10a, from the interconnecting device 10b. Then the setting unit 108 allows the communication device identified by the device identifier received by the communication unit 112 to communicate in the interconnecting device 10a by storing in the storage unit 110 the device identifier received by the communication unit 112.

[0040] If appropriate, the communication unit 112 transmits a device identifier read from a nonvolatile memory to the interconnecting device 10b, which connects to the interconnecting device 10a, so as to allow a communication device identified by the device identifier read from the nonvolatile memory to communicate in the interconnecting device 10b. The communication unit 112 may transmit a device identifier read from a nonvolatile memory to the management apparatus 20, which manages the computer network 100, so as to set to allow a communication device identified the device identifier read from the nonvolatile memory to communicate in the computer network 100.

[0041] The setting unit 108 may set bandwidth of communication, in the interconnecting device 10a, of a communication device identified by a device identifier read from a nonvolatile memory. For example, the setting unit 108 may set a priority order for each of the plurality of connection ports. In another occasion, the setting unit 108

may set upper limitation of bandwidth for each of the plurality of connection ports.

[0042] Each of the holding units 102a, 102b, 102c, 102d, 102e and 102f may correspond to each of the connection ports 116a, 116b, 116c, 116d, 116e and 116f. In other words, the communication controller 114 may restrict communication, in the interconnecting device 10a, of a communication device connected to the connection port 116a based on a device identifier read from a nonvolatile memory held by the holding unit 102a, and may restrict communication, in the interconnecting device 10a, of a communication device connected to the connection port 116b based on a device identifier read from a nonvolatile memory held by the holding unit 102b.

[0043] For example, the reading unit 104 reads the device identifier of the communication device 30a, which is allowed to communicate in the computer network 100, from the nonvolatile memory held by the holding unit 102a. The reading unit 104 also reads the device identifier of the communication device 30b, which is allowed to communicate in the computer network 100, from the nonvolatile memory held by the holding unit 102b.

[0044] Then the setting unit 108 stores in the storage unit 110 the device identifier so as to allow the communication device 30a identified by the device identifier read from the nonvolatile memory held by the holding unit 102a to communicate at the connection port 116a. The setting unit 108 also stores in the storage unit 110 the device identifier so as to allow the communication device 30b identified by the device identifier read from the nonvolatile memory held by the holding unit 102b to communicate at the connection port 116b. Then the communication controller 114 restricts access from a communication device, which is not allowed to communicate in the interconnecting device, based on the device identifier stored in the storage unit 110.

[0045] The communication controller 114 may restrict communication, in the interconnecting device 10a, from the communication devices 30c and 30d connecting to the interconnecting device 10b based on a device identifier read from a nonvolatile memory held by a holding unit of the interconnecting device 10b. The setting unit 108 may set bandwidth of communication at the connection ports 116a, 116b, 116c, 116d, 116e and 116f.

[0046] According to the interconnecting device 10a of the present embodiment, leak of a device identifier in a nonvolatile memory can be prevented since the interconnecting device 10a reads an encrypted device identifier of a communication device from a nonvolatile memory and decode it. Also according to the interconnecting device 10a of the present embodiment, a communication channel in the computer network 100 can be used effectively since the interconnecting device 10a can set bandwidth, in the interconnecting device 10a, of each of communication devices or each of connection ports based on setting information in a nonvolatile memory inserted into the interconnecting device 10a. Also according to the computer network 100 of the present embodiment, a computer network system with high security against illegal access can be built since each of the interconnecting devices restricts access to the respective interconnecting device from a communication device which is not allowed to communicate in the interconnecting devices.

[0047] Fig. 3 shows an example of a data format of a communication control file stored into the storage unit 110. The communication control file includes a connection port number field and a device identifier field. The connection port number field stores the connection port number which is assigned to identify each of a plurality of connection ports in the interconnecting device. The device identifier field stores a device identifier to identify a communication device. For example, the device identifier field stores a MAC address of the communication device.

[0048] In the present embodiment, the connection port number of connection port 116a is 1, the connection port number of connection port 116b is 2, the connection port number of connection port 116c is 3, the connection port number of connection port 116d is 4, the connection port number of connection port 116e is 5, and the connection port number of connection port 116f is 6.

[0049] The communication control file corresponds to each of the plurality of connection ports and stores a device identifier of at least one communication device, the device identifier allowing the communication device to communicate at the corresponding connection port of the plurality of connection ports. For example, the communication controller 114 refers to header information of data received at a designated connection port and allow the communication unit 112 to transmit the data when the

device identifier of the communication device included in the header information and the connection port number to which the communication device connects are consistent with the device identifier and the connection port number stored in the communication control file.

[0050] A nonvolatile memory, which stores a device identifier for identification of a communication device, is inserted by a user of the communication device into one of the holding unit 102a, 102b, 102c, 102d, 102e or 102f, so that a device identifier in a nonvolatile memory is stored in the communication control file. When the nonvolatile memory is removed from one of the holding unit 102a, 102b, 102c, 102d, 102e or 102f by the user, the device identifier stored in the communication control file is deleted.

[0051] The communication controller 114 allows a communication device identified by a device identifier 1A251F33262D to communicate at the connection port 116a (connection port number 1). The communication controller 114 allows a communication device identified by a device identifier 3F3610152A1B to communicate at the connection port 116b (connection port number 2). The communication controller 114 allows a communication device identified by a device identifier 00A0D22A181C to communicate at the connection port 116d (connection port number 4).

[0052] The communication controller 114 allows a communication device identified by a device identifier 00A0D21F253B and a communication device identified by a device identifier 00A0D215361F to communicate at the connection port 116f (connection port number 6). This is the case where the communication device identified by the device identifier 00A0D21F253B and the communication device identified by a device identifier 00A0D215361F connect to the connection ports of the interconnecting device 10b which connects to the connection port 116f.

[0053] According to the interconnecting device 10a of the present embodiment, only access from a designated communication device is allowed at a corresponding connection port by restricting access from a communication device at each of the plurality of connection ports. Consequently, a computer network system with high security against illegal access can be built.

[0054] Fig. 4 shows an example of a configuration of the computer network 100 and a computer network 200. The configuration of the computer network 100 is as same as the configuration depicted in Fig. 1. The computer network 200 includes an interconnecting device 10c, such as a switching hub, which interconnects communication in the computer network 200, and communication devices 30e and 30f which are in communication in the computer network 200. Segment of the computer network 100 is different from segment of the computer network 200 and an interconnecting device 40, such as a bridge or a router, connects the computer network 100 and the computer network 200.

[0055] A user of the communication device 30a inserts a nonvolatile memory into the holding unit 102a of the interconnecting device 10. Then the interconnecting device 10a transmits a device identifier, which identifies the communication device 30a, read from the nonvolatile memory, to the interconnecting device 40 via the interconnecting device 10b so as to allow the communication device 30a to communicate in the computer network 200. Then the interconnecting device 40 allows the communication device 30a identified by the device identifier received from the interconnecting device 10a to communicate in the interconnecting device 40. Consequently, the communication device 30a is allowed to communicate with the communication devices 30e and 30f in the computer network 200 whose segment is different from the computer network 100.

[0056] According to the interconnecting device 10a of the present embodiment, a user of a communication device can be allowed to log into a computer network whose segment is different from segment to which the communication device belongs, by inserting a nonvolatile memory into an interconnecting device which is directly connected to the communication device.

[0057] Fig. 5 shows hardware components in the management apparatus 20. The management apparatus 20 includes a CPU 700, a ROM 702, a RAM 704, a communication interface 706, a hard disk drive 708, a database interface 710, a diskette drive 712 and a CD-ROM drive 714. The CPU 700 controls each section based on program in the ROM 702 and RAM 704. The communication interface 706 communicates with the interconnecting device 10a via a computer network. The

database interface 710 writes data to a database and updates contents of the database.

[0058] The diskette drive 712 reads data or program from a diskette 720 and transmits the data or the program to the communication interface 706. The CD-ROM drive 714 reads data or program from a CD-ROM 722 and transmits the data or the program to the communication interface 706. The communication interface 706 transmits the data or the program from the diskette drive 712 or the CD-ROM drive 714 to the interconnecting device 10a. The database interface 710 connects to various types of databases 724 and transmits and receives data to/from the various types of databases 724.

[0059] Program supplied to the interconnecting device 10a is stored on a recording medium, such as the diskette 720 or the CD-ROM 722, which is provided by a user. The program in the recording medium may be either compressed or decompressed. The program is read from the recording medium, installed on the interconnecting device 10a via the communication interface 706, and executed on the interconnecting device 10a.

[0060] The program stored in the recording medium, that is, the program to be installed on the interconnecting device 10a includes a reading module, a setting module, a decoding module, a transmitting module, a storing module and a communication control module as a functional configuration. Explanation of the modules shall be omitted since each operation, which is performed by the instruction from each of the modules, is identical with that of the corresponding device in the interconnecting device 10a, which has been explained in connection with Figs. 1 to 4.

[0061] Function of some or all of operations of the interconnecting device 10a in all embodiments in the present application can be stored in the diskette 720 or the CD-ROM 720, which is examples of recording media, shown in Fig. 5.

[0062] These programs may be read directly from the recording medium and be executed by the interconnecting device 10a, or may be executed after the programs are installed in the interconnecting device 10a. The programs may be stored either on a single recording medium or a plurality of recording media. The program may be

stored in an encoded form.

[0063] It is possible to use an optical recording medium such as DVD or PD, a magneto-optical recording medium such as Minidisk, a tape medium, a magnetic recording medium or a semiconductor memory such as an IC card or a Miniature Card as a recording medium instead of the diskette or the CD-ROM. A storage device, such as a hard disk or a RAM in a server system on a dedicated communication network or the Internet, may be used as a recording medium and program may be provided to the interconnecting device 10a via the communication network. Such recording media shall be used only for manufacturing the interconnecting device 10a and it is obvious that manufacturing or selling of such recording media, in the course of trade, shall be deemed to be an infringement of a patent right based on this application.

[0064] Although the present invention has been described by way of exemplary embodiments, it should be understood that many changes and substitutions may be made by those skilled in the art without departing from the spirit and the scope of the present invention which is defined only by the appended claims.